使用匯出原則保護 SMB 存取安全

ONTAP 9

NetApp
April 24, 2024

目錄

使用匯出原則保護 SMB 存取安全

如何將匯出原則用於SMB存取

如果SMB伺服器上已啟用SMB存取的匯出原則、則會在控制SMB用戶端對SVM磁碟區的存取時使用匯出原則。若要存取資料、您可以建立允許SMB存取的匯出原則、然後將原則與包含SMB共用的磁碟區建立關聯。

匯出原則會套用一或多個規則、指定允許哪些用戶端存取資料、以及哪些驗證傳輸協定支援唯讀和讀寫存取。您可以設定匯出原則、允許透過SMB存取所有用戶端、用戶端子網路或特定用戶端、並在決定資料的唯讀和讀寫存取時、允許使用Kerberos驗證、NTLM驗證或Kerberos和NTLM驗證進行驗證。

在處理所有套用至匯出原則的匯出規則之後ONTAP 、即可判斷用戶端是否已獲授予存取權限、以及授予何種存取層級。匯出規則適用於用戶端機器、而非Windows使用者和群組。匯出規則不會取代Windows使用者和群組型驗證與授權。匯出規則除了提供共用和檔案存取權限之外、還提供另一層存取安全性。

您只需將一個匯出原則與每個磁碟區建立關聯、即可設定用戶端對磁碟區的存取。每個SVM可包含多個匯出原則。這可讓您針對具有多個磁碟區的SVM執行下列作業：

- 為SVM的每個Volume指派不同的匯出原則、以便個別用戶端存取控制到SVM中的每個Volume。
- 將相同的匯出原則指派給SVM的多個磁碟區、以獲得相同的用戶端存取控制權、而無需為每個磁碟區建立新的匯出原則。

每個SVM至少有一個稱為「預設」的匯出原則、不含任何規則。您無法刪除此匯出原則、但可以重新命名或修改它。SVM上的每個Volume預設都與預設匯出原則相關聯。如果在SVM上停用SMB存取的匯出原則、「預設」匯出原則對SMB存取沒有影響。

您可以設定規則來提供NFS和SMB主機的存取權、並將該規則與匯出原則建立關聯、然後再與包含NFS和SMB主機所需存取之資料的磁碟區建立關聯。或者、如果有些磁碟區只有SMB用戶端需要存取、您可以設定匯出原則、其中的規則僅允許使用SMB傳輸協定存取、而且只使用Kerberos或NTLM（或兩者）進行唯讀和寫入存取驗證。然後、匯出原則會與僅需要SMB存取的磁碟區建立關聯。

如果啟用SMB的匯出原則、且用戶端提出的存取要求不受適用的匯出原則允許、則要求會以拒絕權限的訊息失敗。如果用戶端不符合磁碟區匯出原則中的任何規則、則會拒絕存取。如果匯出原則是空的、則所有存取都會隱含拒絕。即使共用和檔案權限不允許存取、也會發生這種情況。這表示您必須將匯出原則設定為在包含SMB共用的磁碟區上、至少允許下列項目：

- 允許存取所有用戶端或適當的用戶端子集
- 允許透過SMB存取
- 使用Kerberos或NTLM驗證（或兩者）、允許適當的唯讀和寫入存取

深入瞭解 "設定及管理匯出原則"。

匯出規則的運作方式

匯出規則是匯出原則的功能要素。匯出規則會根據您設定的特定參數、將用戶端存取要求與磁碟區相符、以決定如何處理用戶端存取要求。

匯出原則必須包含至少一個匯出規則、才能允許存取用戶端。如果匯出原則包含多個規則、則會依照規則在匯出原則中的顯示順序來處理這些規則。規則順序由規則索引編號決定。如果規則符合用戶端、則會使用該規則的權限、而且不會再處理其他規則。如果沒有符合的規則、用戶端就會被拒絕存取。

您可以使用下列準則來設定匯出規則、以決定用戶端存取權限：

- 傳送要求的用戶端所使用的檔案存取傳輸協定、例如NFSv4或SMB。
- 用戶端識別碼、例如主機名稱或IP位址。

  的最大大小 `-clientmatch` 欄位為 4096 個字元。

- 用戶端用來驗證的安全性類型、例如Kerberos v5, NTL,或AUTH_SYS。

如果規則指定多個準則、用戶端必須符合所有準則、才能套用規則。

範例

匯出原則包含具有下列參數的匯出規則：

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

用戶端存取要求是使用NFSv3傳輸協定傳送、用戶端的IP位址為10.1.17.37。

即使用戶端存取傳輸協定相符、用戶端的IP位址仍位於與匯出規則中指定的子網路不同的子網路中。因此、用戶端比對失敗、此規則不適用於此用戶端。

範例

匯出原則包含具有下列參數的匯出規則：

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

用戶端存取要求是使用NFSv4傳輸協定傳送、用戶端的IP位址為10.1.16.54。

用戶端存取傳輸協定相符、用戶端的IP位址位於指定的子網路中。因此、用戶端配對成功、此規則適用於此用戶端。無論用戶端的安全類型為何、都能取得讀寫存取權。

範例

匯出原則包含具有下列參數的匯出規則：

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`

- `-rwrule krb5,ntlm`

用戶端#1的IP位址為10.1.16.207、使用NFSv3傳輸協定傳送存取要求、並使用Kerberos v5進行驗證。

用戶端#2的IP位址為10.1.16.211、使用NFSv3傳輸協定傳送存取要求、並透過AUTH_SYS進行驗證。

兩個用戶端的用戶端存取傳輸協定和IP位址都相符。唯讀參數允許所有用戶端的唯讀存取權、無論其驗證的安全類型為何。因此這兩個用戶端都能取得唯讀存取權。但是、只有用戶端#1會取得讀寫存取權、因為它使用核准的安全性類型Kerberos v5.x進行驗證。用戶端#2無法取得讀寫存取權。

限制或允許透過**SMB**存取的匯出原則規則範例

這些範例說明如何在啟用SMB存取匯出原則的SVM上、建立限制或允許存取SMB的匯出原則規則。

SMB存取的匯出原則預設為停用。只有在啟用SMB存取的匯出原則時、才需要設定限制或允許透過SMB存取的匯出原則規則。

僅適用於**SMB**存取的匯出規則

下列命令會在名為「'VS1'」的SVM上建立具有下列組態的匯出規則：

- 原則名稱：if1
- 索引編號：1.
- 用戶端比對：僅比對網路192.168.1.0/24上的用戶端
- 傳輸協定：僅啟用SMB存取
- 唯讀存取：使用NTLM或Kerberos驗證的用戶端
- 讀寫存取：使用Kerberos驗證的用戶端

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule krb5,ntlm -rwrule krb5
```

SMB與**NFS**存取的匯出規則

下列命令會在SVM上建立具有下列組態的「」VS1「匯出規則：

- 原則名稱：ifsnfs1
- 索引編號： 2.
- 用戶端配對：符合所有用戶端
- 傳輸協定：SMB與NFS存取
- 唯讀存取：存取所有用戶端
- 讀寫存取：使用Kerberos（NFS和SMB）或NTLM驗證（SMB）的用戶端

- UNIX使用者ID 0對應（零）：對應至使用者ID 65534（通常對應至使用者名稱nobnobody）
- SUID和SGID存取：允許

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifsnfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule
any -rwrule krb5,ntlm -anon 65534 -allow-suid true
```

僅使用**NTLM**匯出**SMB**存取規則

下列命令會在名為「'VS1'」的SVM上建立具有下列組態的匯出規則：

- 原則名稱：ntlm1
- 索引編號：1.
- 用戶端配對：符合所有用戶端
- 傳輸協定：僅啟用SMB存取
- 唯讀存取：僅限使用NTLM的用戶端
- 讀寫存取：僅限使用NTLM的用戶端

> 如果您將唯讀選項或讀寫選項設定為僅限NTL-存取、則必須在用戶端比對選項中使用IP位址型項目。否則、您就會收到 `access denied` 錯誤。這是因為ONTAP 使用主機名稱檢查用戶端存取權限時、使用Kerberos服務主要名稱（SPN-）。NTLM驗證不支援SPN-Name。

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm
-rwrule ntlm
```

啟用或停用**SMB**存取的匯出原則

您可以在儲存虛擬機器（SVM）上啟用或停用SMB存取的匯出原則。您可以選擇使用匯出原則來控制SMB對資源的存取。

開始之前

以下是啟用SMB匯出原則的需求：

- 用戶端在DNS中必須有「'PTTR'」記錄、才能建立該用戶端的匯出規則。
- 如果SVM提供對NFS用戶端的存取、且您要用於NFS存取的主機名稱與CIFS伺服器名稱不同、則需要額外一組「a」和「'PTTR'」的主機名稱。

關於這項工作

在SVM上設定新的CIFS伺服器時、預設會停用SMB存取的匯出原則。如果您想要根據驗證傳輸協定或用戶端IP位址或主機名稱來控制存取、可以啟用SMB存取的匯出原則。您可以隨時啟用或停用SMB存取的匯出原則。

步驟

1. 將權限層級設為進階： `set -privilege advanced`
2. 啟用或停用匯出原則：
   - 啟用匯出原則： `vserver cifs options modify -vserver *vserver_name* -is -exportpolicy-enabled true`
   - 停用匯出原則： `vserver cifs options modify -vserver *vserver_name* -is -exportpolicy-enabled false`
3. 返回管理權限層級： `set -privilege admin`

範例

下列範例可讓您使用匯出原則來控制SMB用戶端對SVM VS1上資源的存取：

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-exportpolicy
-enabled true

cluster1::*> set -privilege admin
```